UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/534,541 | 05/10/2005 | Yukio Tsuruoka | 271813US90PCT | 6985 |

22850 7590 05/12/2010
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

| EXAMINER | |
|---|---|
| VAUGHAN, MICHAEL R | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2431 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 05/12/2010 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

| | | |
|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/534,541 | **Applicant(s)**<br>TSURUOKA ET AL. |
| | **Examiner**<br>MICHAEL R. VAUGHAN | **Art Unit**<br>2431 |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *14 April 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,3-5,7-10,12,14,15 and 17-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1,3-5,15,17-20 and 24* is/are allowed.

6)☒ Claim(s) *7-10,12,14,21-23 and 25* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **4/14/10** has been entered.

Claims 7, 12, 14, 21, and 22 have been amended. Claims 1, 3-5, 7-10, 12, 14, 15, and 17-25 are pending.

## *Response to Amendment*

### *Claim Objections*

Claim 14 is objected to because of the following informalities:

The key information is defined for thr second time in the ticket reception means clause. The session secret key in the last clause lacks antecedent basis.

### *Claim Rejections - 35 USC § 101*

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 22 and 23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 22 and 23 comprise computer readable medium. Computer readable medium include signals. Signals are not a statutory class of invention. In order to overcome this interpretation, the claim should be amended to only include "non-transitory" computer readable-medium. There is support for this amendment because the original disclosure does not preclude the non-transitory types of computer readable medium.

## ***Response to Arguments***

Applicant's arguments with respect to claims 7, 12, 14, 21, and 22 have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7-10, 14, 21, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Newcombe** (US 2003/0172269 A1) in view of **Sudia** (US 2005/0114653).

As per claim 7, Newcombe teaches the limitation of an “authentication server in an authentication system in which an authentication of a user utilizing a user terminal is performed through the user terminal by an authentication server and a request is made to an application server to provide a service on the basis of the authentication” (Fig. 1; page 2, paragraph 0025) as the system includes a client that desires access to a content server, application server, or the like. The authentication manager includes an application authentication server and ticket granting server.

Further, Newcombe teaches the limitation of “a reception means for receiving an authentication request inclusive of a user authentication information [pre-authenticator; timestamp encrypted by salted password (0057)] transmitted from the user terminal” as Application Authentication Server (AAS) is configured to authenticate a user. Where, (page 4, paragraph 0052) clients are enabled to request access to servers, such as content servers by requesting content tickets from AAS.

Furthermore, Newcombe teaches the limitation of “an authentication means to which the user authentication information of the received authentication request is input and which authenticates the user on the basis of the user authentication information and providing a signal indicating a successful authentication upon a successful authentication” (page 5, paragraph 0064) as Authentication Server (AS) determines the user is a valid user and provides client with a Ticket Granting Ticket. Where AS is a part of AAS (page 4, paragraph 0054) and (page 10, paragraph 0115) a signal is provided that indicates whether the client is authentic or not.

Newcombe teaches "an address allocating means for allocating an address to the user terminal in response to an input of the signal indicating a successful authentication of the user" as part of an initial challenge/response, protocol negotiation, or the like, the authentication server may send to the client the client's remote IP address (0094)

Additionally, Newcombe teaches authentication information generating means for generating information-for-authentication using at least the allocated address and the key information [modified authenticator includes IP address encrypted with session key].

In addition, Newcombe teaches the limitations of "a ticket issuing means for issuing a ticket containing the allocated address, and the information-for-authentication" (0064-67).

Newcombe teaches the application server conducting authentication for providing services to the user terminal based on the ticket (0048).

Newcombe teaches "a ticket transmitting means to which the ticket is input and which transmits the ticket to the user terminal" (page 4, paragraph 0044) as Application Authentication Server (AAS) is configured to provide the authenticated user one or more content tickets that enables authenticated user to access one or more content servers.

Newcombe is silent in teaching the key information, sent to the server from the user, represents a public key and that the ticket contains the key information. Sudia teaches a similar authentication system in which a user sends its public key certificate to an authentication server during the authentication process (Abstract; 0067; and 0053). Therefore the public key located in the certificate is sent to the server along with the other authentication information (login ID/password). The use of public key certificates is well known in the art to prove that a user is who she proclaims to be. The correspondence between user authentication information and the public key help guarantee that a user is not masquerading as someone else. Sudia establishes this correspondence by including the key information in the ticket it creates for the user (0069). Sudia places information from the user's certificate (public key) into the ticket to securely link the ticket data to the client's public key certificate (0069). This creates a bond between the ticket and the user to prove authenticity to the application server. The application server can trust the ticket is authentic and belongs to the user who is seeking services. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results. Including a public key in the ticket granting process was known in the art. A ticket containing the allocated address and key information guarantees a correspondence between the user, the allocated address, and the key information. A user presenting the ticket as shown in Newcombe ties the user to an IP address. This is created by the AS signing a ticket with the IP address as part of the data. As Sudia teaches, placing the user's public key into the ticket ties the user to a particular public key certificate. Newcombe guarantees a correspondence between the user and the allocated address, while Sudia guarantees a correspondence between the user and the key information (public key). Therefore the combination of Newcombe and Sudia guarantees a correspondence between the user, the key information, and the allocated address.

With respect to claim 8, Newcombe teaches the limitation of “an authentication information generating means for generating an authentication information for information which includes at least the allocated address using a shared secret key which is beforehand shared between the authentication server and the application server” (page 4, paragraph 0044) as Application Authentication Server (AAS) is configured to provide the authenticated user one or more content tickets that enables authenticated user to access one or more content servers. The content ticket includes (page 4, paragraph 0048) the client’s local and remote IP addresses. Furthermore, (page 5, paragraph 0065) the client readable portion [of the ticket] is signed with the private key of the authentication server.

With respect to claim 9, Newcombe teaches the limitation of “the authentication server comprises a user identifier allocating means for allocating a user identifier which corresponds to the authenticated user in response to the authentication request for a successful authentication of the user” (page 4, paragraph 0057) as Authentication Server (AS) is enabled to authenticate a user.

In addition, Newcombe teaches the limitations of “authentication information generating means is configured to process the information including the allocated address, the key information, and the user identifier to produce information for authentication and the ticket issuing means is configured to combine at least the information for authentication, the allocated address, the key information and the user identifier to form the ticket" (0025) and "and a ticket transmitting means to which the ticket is input and which transmits the ticket to the user terminal" (page 4, paragraph 0044) as Application Authentication Server (AAS) is configured to provide the authenticated user one or more content tickets that enables authenticated user to access one or more content servers. The content ticket includes (page 4, paragraph 0048) the client's local and remote IP addresses.

As per claim 10, Newcombe teaches the user identifier allocating means is configured to encrypt information which directly identifies the user by using an identifier generating secret key of the authentication server to produce the user identifier (0065).

As per claim 14, Newcombe teaches a user terminal in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication (0052), comprising:

a key information generating means to which an authentication purpose shared secret key (hash/salted user password) which is shared with the application server and a random number (timestamp) which changes each time a session is established are input and which generates a key information (encrypted timestamp, encrypted with the salted password and IP address) by processing the random number by the authentication purpose shared secret key (0057);

a user authentication information transmitting means which is configured to transmit to the authentication server the key information together with the user authentication information for authentication by the authentication server (pre-authentication sent to server; 0057);

a ticket reception means for receiving a ticket transmitted from the authentication server (0064), said ticket containing an address (IP address; 0067) allocated by the authentication server (0094) and information-for-authentication produced by the authentication server based on at least the allocated address [modified authenticator includes IP address; 0067];

the application server conducting authentication for providing services to the user terminal based on the ticket (0048);

a source address set-up means to which the received ticket is input and which sets up the allocated address contained in the ticket as a source address of each packet to be transmitted to the application server [as part of an initial challenge/response, protocol negotiation, or the like, the authentication server may send to the client the client's remote IP address (0094)];

a session establishing means to which the ticket is input and which transmits a first packet including the ticket to the application server for establishing a session with the application server (0047);

a service request means for transmitting a second packet representing a service request to the application server through the established session (0046);

and a packet cryptographic processing means to which a packet to be transmitted from the user terminal and the session secret key (0065) are input and which applies a processing to the transmitted packet which guarantees that there is no forgery in the packet by the session secret key [tickets contain session keys and session key are used for encrypting message; 0032].

Newcombe is silent in explicitly teaching the key information is sent back in the ticket. Sudia teaches a similar authentication system in which a user sends its public key to an authentication server during the authentication process (Abstract; 0067; and 0053) so that the server may inject the public key into the signed ticket (0069). This establishes a relationship between key information which the user knows (and can produce because she knows the password) and the ticket because the key information has been sealed in it by the server. The method of sending key information and having it sealed into a ticket establishes a correspondence between the user and the key information. The application server can trust the ticket is authentic and belongs to the user who is seeking services. The authenticity of the user is shown by the user being able to reproduce data that was sealed in the ticket by the server. A user that can perform this reproduction must have been the same user that received the ticket in the first place. Newcombe uses the knowledge of a shared secret key (user's password) bound to a timestamp and IP address to prove the user is who she says she is. This is another example of key information, and it could have been used in the same manner as taught by Sudia. The claim is obvious because one of ordinary skill in the art can substitute known methods which produce predictable results. A ticket containing the allocated address and key information guarantees a correspondence between the user, the allocated address, and the key information. A user presenting the ticket from the IP address included in the ticket as shown in Newcombe ties the user to an IP address. As Sudia teaches, placing the key information into the ticket ties the user to key information. Newcombe guarantees a correspondence between the user and the allocated address, while Sudia guarantees a correspondence between the user and the key information. Therefore the combination of Newcombe and Sudia guarantees a correspondence between the user, the key information, and the allocated address.

With respect to claim 21, it is rejected in view of the reasons stated in the rejection of independent claim 7.

As per claim 25, Newcombe teaches the authentication server has a secret key and a public key for digital signature (0029), and said ticket issuing means comprises: an authentication information generating means for computing a digital signature on the information including at least the allocated address using the secret key to produce the information for authentication so that the application server can verify the presence or absence of any forgery in the information for authentication in the ticket using the public key of the authentication server (0030 and 0065-0066).

Claims 12 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Newcombe** (US 2003/0172269 A1) in view of **Sudia** (US 2005/0114653) and in view of **Medvinsky** (US 2003/0163693).

As per claim 12, Newcombe teaches a user terminal in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication (0052), the user terminal having a pair of a public key and a private key (0029), comprising:

A key information generating means to which the public key of the user terminal is input and which generates a key information representing the public key of the user terminal (0027, 0029; RSA);

A user authentication information transmitting means configured to transmit user authentication information (timestamp encrypted with salted password) to the authentication server (0057);

a ticket reception means for receiving a ticket transmitted from the authentication server (0064), said ticket containing an address (0067) allocated by the authentication

(00994), and information-for-authentication produced by using at least the allocated address and the key information [modified authenticator includes IP address encrypted with session key; 0067];

the application server conducting authentication for providing services to the user terminal based on the ticket (0048);

a source address set-up means to which the received ticket is input and which sets up the allocated address contained in the ticket as a source address of each packet to be transmitted to the application server [as part of an initial challenge/response, protocol negotiation, or the like, the authentication server may send to the client the client's remote IP address (0094)];

a session establishing means to which the ticket is input and which transmits a first packet including the ticket to the application server for establishing a session with the application server (0047) using the session secret key (0032);

a service request means for transmitting a second packet representing a service request to the application server through the established session (0046);

and a packet cryptographic processing means to which a packet to be transmitted from the user terminal and the session secret key (0065) are input and which applies a processing to the transmitted packet which guarantees that there is no forgery in the packet by the session secret key [tickets contain session keys and session key are used for encrypting message; 0032].

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Arnold into the system of Newcombe to allow the AAS to keep full control of the IP address assignment process in view of the limited pool of available IP addresses.

Newcombe is silent in explicitly teaching session keys are created using the private and public keys of the user terminal and the application server. Newcombe does teach using a session key between the client and server and that any algorithm could be used. The algorithm used in the claim is a well known Diffie-Hellman type (e.g. IKE, Oakley) key exchange. Medvinsky teaches this same type of key exchange with the use of tickets (0013). As taught by Medvinsky, it is necessary to send the public key of the client to the server in order to complete a Diffie-Hellman type key exchange (0030-31). The claim is obvious because one of ordinary skill can substitute known methods which produce predictable results. The combination of Medvinsky produces a well known and secure key exchange.

Newcombe is silent in teaching the key information, sent to the server from the user, represents a public key and that the ticket contains the key information. Sudia teaches a similar authentication system in which a user sends its public key certificate to an authentication server during the authentication process (Abstract; 0067; and 0053). Therefore the public key located in the certificate is sent to the server along with the other authentication information (login ID/password). The use of public key certificates is well known in the art to prove that a user is who she proclaims to be. The correspondence between user authentication information and the public key help guarantee that a user is not masquerading as someone else. Sudia establishes this correspondence by including the key information in the ticket it creates for the user (0069). Sudia places information from the user's certificate (public key) into the ticket to securely link the ticket data to the client's public key certificate (0069). This creates a bond between the ticket and the user to prove authenticity to the application server. The application server can trust the ticket is authentic and belongs to the user who is seeking services. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results. Including a public key in the ticket granting process was known in the art. A ticket containing the allocated address and key information guarantees a correspondence between the user, the allocated address, and the key information. A user presenting the ticket as shown in Newcombe ties the user to an IP address. This is created by the AS signing a ticket with the IP address as part of the data. As Sudia teaches, placing the user's public key into the ticket ties the user to a particular public key certificate. Newcombe guarantees a correspondence between the user and the allocated address, while Sudia guarantees a correspondence between the user and the key information (public key). Therefore the combination of Newcombe and Sudia guarantees a correspondence between the user, the key information, and the allocated address.

With respect to claim 22, it is rejected in view of the same reasons as stated in the rejection of independent claim 12.

### ***Allowable Subject Matter***

Claims 1, 3-5, 15, 17-20, and 24 are allowed.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431